



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10334008 A**(43) Date of publication of application: **18.12.98**

(51) Int. Cl. **G06F 13/00**
G06F 12/14
G06F 15/00

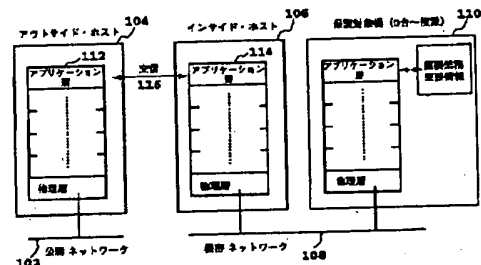
(21) Application number: **09127079**(22) Date of filing: **16.05.97**(71) Applicant: **INTERNATL BUSINESS MACH
CORP <IBM>**(72) Inventor: **NEMOTO KAZUO**(54) **NETWORK SECURITY SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To secure a high security in a system connected to a network.

SOLUTION: An outside host 104 is connected to an external network 102. A 1st connection program 112 for providing the security of the network 102 is stored in the host 104. The host 104 is connected to an inside host 106 through an exclusive transmission line 116. A 2nd connection program 114 is stored also in the host 106. The 1st and 2nd connection programs 112, 114 are respectively constituted of an application level program and a driver program for driving an exclusive transmission line. Communications can be attained only between the two connection programs 112, 114 and intrusion from the external can be prevented by executing communication only between two connection programs 112, 114. In addition, another part in the system can be prevented from being accessed.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-334008

(43) 公開日 平成10年(1998)12月18日

(51) Int.Cl.⁸
G 0 6 F 13/00 3 5 1
12/14 3 1 0
15/00 3 3 0

F I
G 0 6 F 13/00 3 5 1 M
12/14 3 1 0 N
15/00 3 3 0 A

審査請求 未請求 請求項の数5 O L (全 8 頁)

(21) 出願番号 特願平9-127079
(22) 出願日 平成9年(1997)5月16日

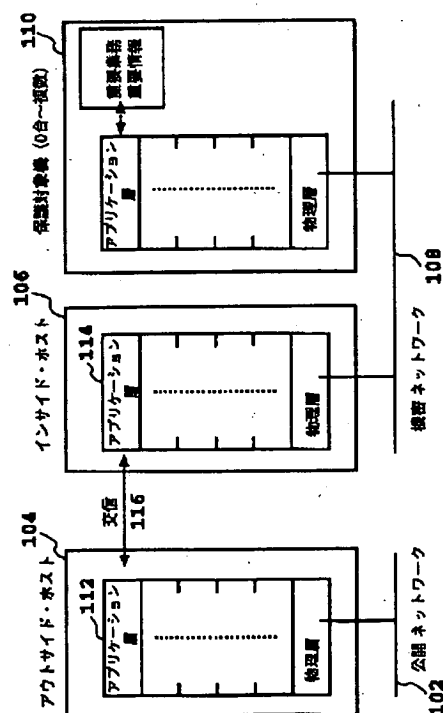
(71) 出願人 390009531
インターナショナル・ビジネス・マシー
ズ・コーポレーション
INTERNATIONAL BUSIN
ESS MASCHINES CORPO
RATION
アメリカ合衆国10504、ニューヨーク州
アーモンク (番地なし)
(72) 発明者 根本 和郎
神奈川県大和市下鶴間1623番地14 日本ア
イ・ビー・エム株式会社 大和事業所内
(74) 代理人 弁理士 坂口 博 (外2名)

(54) 【発明の名称】 ネットワーク・セキュリティ・システム

(57) 【要約】

【課題】 ネットワークに接続されたシステムにおける高度のセキュリティの確保。

【解決手段】 外部からのネットワーク102に、アウトサイド・ホスト104が接続されている。このホスト104には、ネットワークのセキュリティを提供する第1接続プログラム112が実装されている。そして、このアウトサイド・ホストは、インサイド・ホスト106に専用の伝送路116を介して接続されている。このインサイド・ホストにも第2接続プログラム114が実装されている。この2つの第1と第2の接続プログラム112および114は、アプリケーション・レベルのプログラムおよび専用の通信路を駆動するドライバ・プログラムから構成されている。そして、2つの接続プログラム間のみで交信することで、外部からの侵入を防ぐことができる。また、システム内の他の部分にアクセスされることを防ぐことができる。



【特許請求の範囲】

【請求項1】 外部のネットワークと接続されているシステムにおいて、

外部ネットワークとの間でヘッダ付きパケットを送受信する第1のコンピュータと、

前記第1のコンピュータと専用の通信路で接続されている第2のコンピュータとを含み、

前記第1のコンピュータは、前記専用通信路を介して前記ヘッダ付きパケットからヘッダを落としたパケットを前記第2のコンピュータに送信し、前記第2のコンピュータから前記専用通信路を介した受け取ったパケットにヘッダを付加して前記外部ネットワークに対して送信することを特徴とするネットワーク・セキュリティ・システム。

【請求項2】 請求項1記載のネットワーク・セキュリティ・システムにおいて、前記通信路は、調歩式伝送により構成されていることを特徴とするネットワーク・セキュリティ・システム。

【請求項3】 請求項1または2記載のネットワーク・セキュリティ・システムにおいて、前記第2のコンピュータは、前記ヘッダを落としたパケットが予定のフォーマットであるか否かを判断することを特徴とするネットワーク・セキュリティ・システム。

【請求項4】 請求項1ないし3いずれか記載のネットワーク・セキュリティ・システムにおいて、前記第2のコンピュータは、第2のコンピュータと接続されているサーバーに対して、受信した前記パケットに含まれるデータを送信することを特徴とするネットワーク・セキュリティ・システム。

【請求項5】 請求項1ないし3いずれか記載のネットワーク・セキュリティ・システムにおいて、前記第2のコンピュータは受信した前記パケットに含まれるデータに対する処理を行い、処理結果を第1のコンピュータに送信することを特徴とするネットワーク・セキュリティ・システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークに接続されたコンピュータ・システムにおいて、外部から機密を保持しなければならない内部システムに侵入されないようにしたネットワーク・セキュリティ・システムに関する。

【0002】

【従来の技術】従来において、外部のネットワーク・システム例えばインターネットに接続されたコンピュータ・システムにおいて、外部からの侵入を防ぐシステムとしては、ファイアウォール・システムが知られている。このシステムは、ファイアウォールのプログラムを実装した要塞システムを設けることで、外部からの侵入を防ぐものである。このファイアウォールを二重に用いてい

る2つの要塞ホストを使用したシステムも知られている。

【0003】この2つの要塞ホストを使用したシステムを、図7および図8を用いて説明する。

【0004】図7において、外部のネットワーク（インターネット）702に内部ネットワークを接続しているシステムを示している。インターネット702には、スクリーニング・ルーター704を介して内部ネットワークが接続されている。スクリーニング・ルーター704は、外部ネットワーク702から受信した内部ネットワーク向けのすべてのトラフィックを、要塞ホスト708の外側のネットワーク706に設定されている。また、スクリーニング・ルーター704は、トラフィックを要塞ホスト708に送る前にフィルタ・ルールを適用して、フィルタ・ルールをパスしたトラフィックのみが要塞ホスト708に送られる。

【0005】アウトサイド・ネットワーク706は、非武装地帯（Demilitarized Zone: DMZ）を形成している。このアウトサイド・ネットワークは、ファイアウォールを搭載した要塞ホスト708によって守られていない。外部ネットワーク702からのトラフィックはアウトサイド要塞ホスト708を介して、プライベート・ネットワーク710に転送される。このプライベート・ネットワークは、ファイアウォールにより一応の機密性を保っているため、外部からアクセスするためのホストや、内部のあまり機密性を要しないホストをこの段階に設置することができる。

【0006】より機密性の高いホストは、ファイアウォールを実装しているインサイド要塞ホスト712を介してプライベート・ネットワークに接続されているインサイド・ネットワーク714に接続する。このインサイド・ネットワークは、二重のファイアウォールにより守られているので、例えば電子署名のキー等の厳重な機密性を要するものを提供しているホストを接続する。

【0007】

【発明が解決しようとする課題】このように、二重に守られているインサイド・ネットワークでは、二重であることにより強度はあげているが、二重化により特別な機能を提供はしておらず、通常のファイアウォールのプログラムを利用している限り限界がある。それは、ファイアウォールのプログラムが複雑であることや、アプリケーション・レベルで実行されていることに起因している。図7にその様子を示している。外部ネットワーク702からのトラフィックは、スクリーニング・ルーター704を介して、アウトサイド要塞ホスト708へと転送される。それから、インサイド要塞ホスト712を介してインサイド・ネットワーク714へと再度転送される。要塞ホスト708および要塞ホスト712には、ファイアウォールのプログラム716および718がアプリケーションの層で実装されており、この部分で外部か

らの侵入を防いでいる。

【0008】そして、下位層の実装は、通常OSと同等のレベルで行われている。この部分は、ユーザにとってはブラックボックスとなっている。そのため、この部分に外部からのアクセスに対して弱い部分があっても、通常のユーザは認知できず、気がついたときには、手遅れとなることも想定される。

【0009】この様な例としては、例えば、OSのバグ、ハードウェアの故障、各種ソフトウェアの設定ミス等がある。この様な原因で外部アクセスについての欠陥が生じた場合、オープン故障（動かなくなる）ならよいが、ショート故障（データが素通しで流れる）のときは重大なセキュリティ上の問題が生じる。

【0010】このようなショート故障や、悪意によってファイアウォール・サーバーが汚染された場合には、例えばインターネットで用いられているプロトコルであるTCP/IPのヘッダに含まれる宛先IPアドレスやサービス・タイプ等は、フェイク可能であり、ドライバ・レベル（下位層）のチェックでは、不十分な場合もあった。

【0011】一方、OSに依存しないファイアウォールを開発することは、OSレベルのコーディングを必要とし、不可能ではないにしても多大な労力および費用を要する。

【0012】本発明は、このようなファイアウォールの本質的な部分の欠点を有さず、セキュリティの高いネットワーク・セキュリティ・システムを提供することを目的としている。

【0013】

【課題を解決するための手段】上記目的を達成するために、本発明は、外部のネットワークと接続されているシステムにおいて、外部ネットワークとの間でヘッダ付きパケットを送受信する第1のコンピュータと、前記第1のコンピュータと専用の通信路で接続されている第2のコンピュータとを含み、前記第1のコンピュータは、前記専用通信路を介して前記ヘッダ付きパケットからヘッダを落としたパケットを前記第2のコンピュータに送信し、前記第2のコンピュータから前記専用通信路を介した受け取ったパケットにヘッダを付加して前記外部ネットワークに対して送信することを特徴とするネットワーク・セキュリティ・システムである。

【0014】また、前記通信路は、調歩式伝送により構成することができる。

【0015】前記第2のコンピュータは、前記ヘッダを落としたパケットが予定のフォーマットであるか否かを判断している。

【0016】前記第2のコンピュータは、第2のコンピュータと接続されているサーバーに対して、受信した前記パケットに含まれるデータを送信することができる。

【0017】前記第2のコンピュータは、受信した前記

パケットに含まれるデータに対する処理を行い、処理結果を第1のコンピュータに送信してもよい。

【0018】このように、本発明の構成によれば、簡単な構成でセキュリティ強度の高いシステムを構築することができる。

【0019】

【発明の実施の形態】本発明の実施形態を、図面を参照して詳細に説明する。

【0020】図1は、本発明の実施の形態を説明するための図である。

【0021】図1において、外部からのアクセスが容易なネットワーク（公開ネットワーク）102に、アウトサイド・ホスト104が接続されている。このホスト104には、本発明のネットワークのセキュリティを提供する第1接続プログラム112が実装されている。そして、このアウトサイド・ホストは、インサイド・ホスト106に専用の伝送路116を介して接続されている。このインサイド・ホストにも第2接続プログラム114が実装されている。この2つの第1と第2の接続プログラム112および114は、アプリケーション・レベルのプログラムおよび専用の通信路を駆動するドライバ・プログラムから構成されている。そして、2つの接続プログラムが通信路を占有するかたちで交信することで、外部からの侵入を防ぐことができる（通常のネットワークにおいては、占有されておらず、多重に使用されている）。また、システム内の他の部分にアクセスされることを防ぐことができる。この第1接続プログラム112および第2接続プログラム114については、後で詳しく説明する。

【0022】インサイド・ホストはセキュリティが確保されているので、これに接続されている内部のネットワーク108は、機密ネットワークである。機密ネットワーク108には、外部からの侵入を保護すべき対象である重要な業務を行っており、重要な情報を有しているホスト110が接続されている。なお、保護対象機110は、接続プログラム106を実装しているインサイド・ホストで兼ねることもできる。この場合は、内部でのネットワーク接続された保護対象のホストがなくてもよい。

【0023】さて、接続プログラム112および114について、図2を用いてさらに具体的に説明する。図2は、双方向のシリアル・ポートで接続し、調歩式伝送で交信している例を示している。図2において、アウトサイド・ホスト104とインサイド・ホストとの間を、ポート202およびポート204で接続している。このシリアル・ポート202およびポート204は2つの接続プログラムに専用となっており、この接続プログラムに含まれるこのポート専用のシリアル・ポート・デバイス・ドライバにより物理的にアクセスされる。このように外部から専用で接続し、しかも、機密ネットワーク10

8を介して接続される外部からのアクセス対象である認証サーバー110等の保護対象のホストには、接続プログラムによりチェックを十分におこなってからアクセスすることが可能であるので、十分なセキュリティを確保することができる。

【0024】この専用のシリアル・ポートにアクセスするためのシリアル・ポート・デバイス・ドライバは、簡単な構成なので自作しても、標準のドライバをテストして使用してもよい。

【0025】従って、この接続はシステム外部からはアクセスすることができず、アウトサイド・ホストの特権ユーザであっても操作できない。また、専用のデバイス・ドライバを使用しているので、従来のファイアウォールを用いた場合と異なり、OS等のバグによるアクセスの穴がない。そして、この専用の接続プログラムや専用のポートや接続線が壊れるときは、2ヶ所に分散しているため、必ず動かなくなる方向である。

【0026】また、外部からアクセスされる特定のサーバー例えば暗号を解読用のキーを発行する認証サーバー110のみにアクセスするための接続にのみこのポートによる接続を用いると、宛先情報が必要なく、その上、その認証サーバー110へのアクセス独特のチェックができ、より機密性が高まる。

【0027】アウトサイド・ホストに実装されている第1接続プログラムは、例えば、上述のように、認証サーバーのみに使用している場合は、宛先（認証サーバー）が決まっており、輻輳制御が必要ない（他へのアクセスがないため）ので、データのみを必要最小限の制御情報（例えば、パリティビット等）を付与して送ればよい。また、この様に認証サーバー専用である場合は、送信するデータ量の少ないのでデータ転送速度もそれほど速い必要はない。

【0028】この第1と第2の接続プログラムの動作について、図3および図4を用いて詳しく説明する。図3および図4では、暗号解読用のキーを発行している認証サーバー110専用に関信を行う場合で説明している。

【0029】図3には、第1と第2の接続プログラムをアウトサイド・ホスト104とインサイド・ホスト106に実装した場合の構成が示されている。アウトサイド・ホスト104は、ユーザ・インタフェース機304に接続されている。ユーザ・インタフェース機304は、外部ネットワーク302に接続されており、外部からのアクセス者に対してホームページ等のユーザ・インタフェースを提供している。

【0030】第1および第2の接続プログラムにはそれぞれ、送信側としてAクライアント(A-client)とCクライアント(C-client)を有し、受信側としてBサーバー(B-server)とDサーバー(D-server)を有している。

【0031】アウトサイド・コンピュータ104のA-

クライアントは、外部ネットワークと接続されているユーザ・インタフェース機304から送られてきた、例えばTCP/IPプロトコルのヘッダを有しているパケットを受信する。次に、Aクライアントは、パケットからヘッダを取り除いて必要なデータのみを調歩式データに変換し、シリアルポートを介してインサイド・ホスト106のBサーバーに送る。Bサーバーは、認証サーバーのクライアント側（認証クライアント）として、認証サーバー110上のキーを管理しているプログラムである認証サーバー110にデータを送信する。

【0032】認証サーバー110では、それが正当なキー発行要求であるならば、暗号解読用のキーを発行して、そのキー・データを認証クライアントであるインサイド・ホスト106に送る。受信した第2接続プログラムのCクライアントは、アウトサイド・ホスト104のDサーバーに調歩式データとしてキー・データをシリアルポートを介して送る。受信したDサーバーは、プロトコルで必要なヘッダをまた付与して、ユーザ・インタフェース機304にキー・データを送る。なお、インサイド・ホスト106と認証サーバー110との間には、通常の通信で送られており、プロトコル上ヘッダが必要なら、インサイド・ホスト106内のBサーバーが付与し、また、Dサーバーがそのヘッダを取り除いている。

【0033】第1および第2接続プログラムの処理について、データの流れを中心に図4を用いてさらに詳細に説明する。

【0034】図4において、具体的には、試用プログラムを使用したユーザーが、試用後に正式版であるプログラムを使うために、暗号化されたいる製品を、CD-ROMやテープ等から解読してインストールするためのキーをインターネット経由で得ることを想定している。

【0035】インターネットからアクセスしたユーザーは、ユーザ・インタフェース機304における解読キーを得るために、WWWのページにアクセスして画面の指示によりユーザID等を入力する。これはREQデータとして、ユーザ・インタフェース機304からアウトサイド・ホスト104に送られる。REQデータの形式は例えば、図4(b)に示す形式である。アウトサイド・ホストの第1接続プログラムは、REQデータを受け取ると送られたパケットからヘッダを取り除いて、自分自身のキューに入れる。第1接続プログラムは、REQデータをキューから受信の順番に、シリアル・ポートを介してインサイド・ホスト106の第2接続プログラムに送る。そして、キューの中の送ったREQデータに対して、キー作成中のフラグをたてる。

【0036】送られてきたREQデータは、第2接続プログラムにおいて、データのフィールド検査を行う。これは図4(b)において、ユーザID、取引ID、商品IDの各々が決められた属性（例えば、数字等の文字種

や桁数)であるかの形式に関するチェックする。そして、正しい場合は自分自身のキューに入れる。正しくない場合はその旨第1接続プログラムにシリアル・ポートを介して伝える。

【0037】インサイド・ホスト106の第2接続プログラムは、形式的に正しいREQデータを認証サーバー110に送るとともに、キー作成中のフラグをたてる。

【0038】認証サーバー110は、送られてきたREQデータを検証し、その結果、確認がとれた場合は、キーを発行して、インサイド・ホスト106に発行したキーのデータを送る。検証の結果、キーが発行できない場合はその旨返送する。

【0039】インサイド・ホスト106の第2接続プログラムでは、キー・データが送られてきたら、対応するフラグをたてたREQデータを消去する。送られてきたキー・データをシリアル・ポートを介してアウトサイド・ホスト104に送る。一定時間待って、送ったREQデータに対する応答がない場合には、そのREQデータを認証サーバー110に再送する。

【0040】アウトサイド・ホスト104の第1接続プログラムは、キー・データをシリアル・ポートを介して第2接続プログラムから受け取ると、対応するREQデータを消去して、キー・データを必要なヘッダを付与してユーザ・インタフェース機304に送る。

【0041】このように、アウトサイド・ホスト104とインサイド・ホスト106との間では、不必要なネゴシエーションは行っていない。これは、ネゴシエーションを行うことにより、この間のインタフェースのプロトコルが複雑になり、セキュリティ強度が下がるからである。

【0042】なお、上記の実施形態において、データのチェックをインサイド・ホスト上の第2接続プログラムにおいて行ったが、第1接続プログラムで行うこともできる。

【0043】インサイド・ホスト106は、認証サーバー110と兼用できる。この場合は、インサイド・ホスト106に認証サーバー110のためのプログラムを実装すればよい。インサイド・ホスト上の第2接続プログラムは、受信したデータを認証サーバー110に転送するのではなく、自機の認証サーバー・プログラムに送

【0044】また、アウトサイド・ホストとユーザ・インタフェース機も兼用することができる。

【0045】上述の図2～図4の説明においては、認証サーバーが1つのみの場合を説明したが、図5に示すように、認証サーバーを2つ以上用いることも可能である。この場合は、第2接続プログラムにおいて、例えば商品IDによりREQデータの送り先を指定する必要がある。

【0046】また、上記で説明したような接続形態を用

いて、図6に示すように、プロトコル層の中間で送受信する様な構成とすることもできる。このような構成とすると、プロトコルの解釈を2つのホスト機602および604で行うことができるので、セキュリティ強度を高めることが可能となる。このような場合の応用としてはルータ等がある。

【0047】上記のプログラムでその機能を実行している部分に関して、それを記録媒体上に格納し、それをコンピュータ・システムで読み出すことにより、本発明を実施することもできる。この記録媒体には、フロッピー・ディスク、CD-ROM、磁気テープ、ROMカセット等がある。

【0048】

【発明の効果】上記の説明のように、本発明の構成を使用すると、外部とネットワークで接続されたシステムにおいて、簡単な構成でセキュリティ強度の高いシステムを構築することができる。

【図面の簡単な説明】

【図1】本発明の実施形態を示す図である。

【図2】本発明の実施形態を示すブロック図である。

【図3】本発明の詳しい実施形態を示すブロック図である。

【図4】本発明の実施形態のデータの流れを示すブロック図である。

【図5】本発明の詳しい実施形態を示すブロック図である。

【図6】本発明の詳しい実施形態を示すブロック図である。

【図7】従来のセキュリティ・システムを示す図である。

【図8】従来のセキュリティ・システムを示す図である。

【符号の説明】

102 公開ネットワーク

104 アウトサイド・ホスト

106 インサイド・ホスト

108 機密ネットワーク

110 保護対象機

112 第1接続プログラム

114 第2接続プログラム

116 伝送路

302 公開ネットワーク

304 ユーザ・インタフェース機

602 外側コンピュータ

604 内側コンピュータ

702 インターネット

704 スクリーニング・ルーター

706 アウトサイドDMZネットワーク

708 アウトサイド要塞ホスト

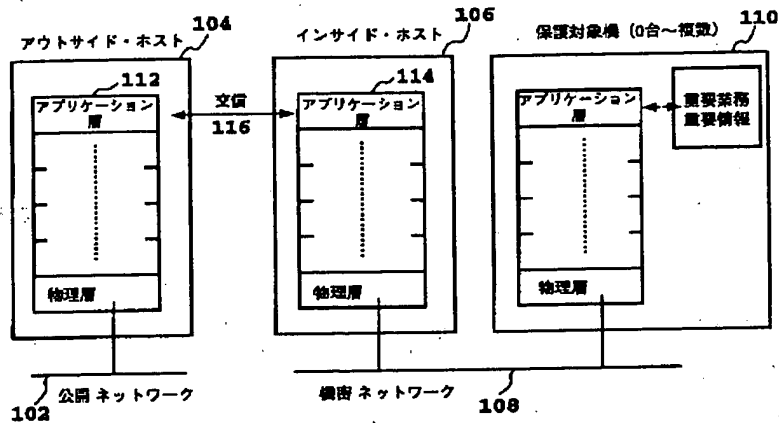
710 インサイドDMZネットワーク (プライベート

・ネットワーク)

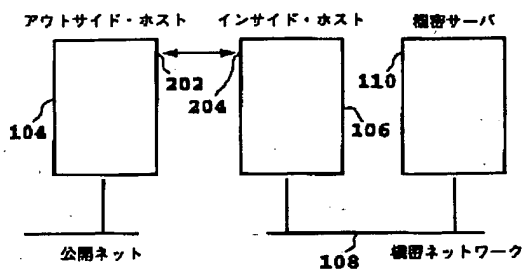
714 インサイド・ネットワーク

712 インサイド要塞ホスト

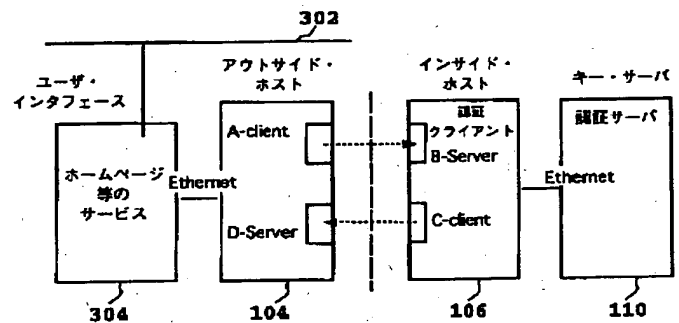
【図1】



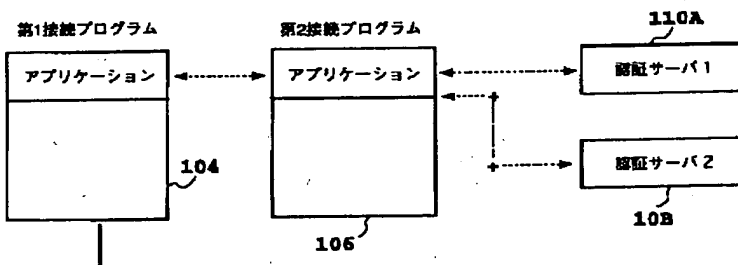
【図2】



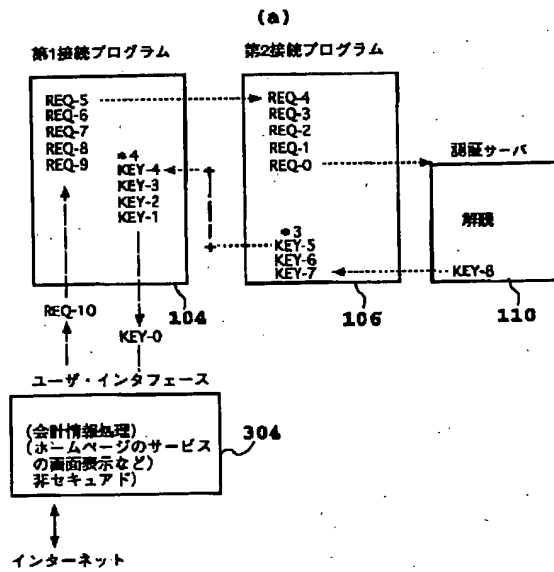
【図3】



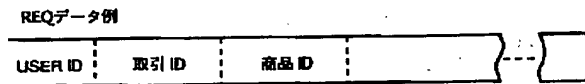
【図5】



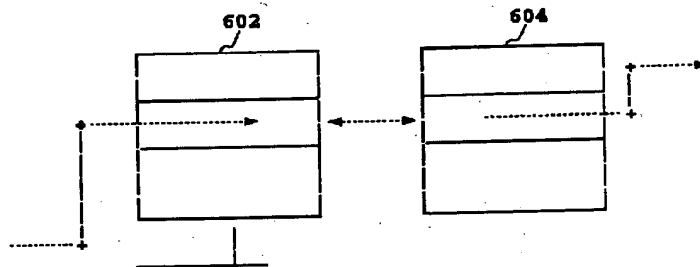
【図4】



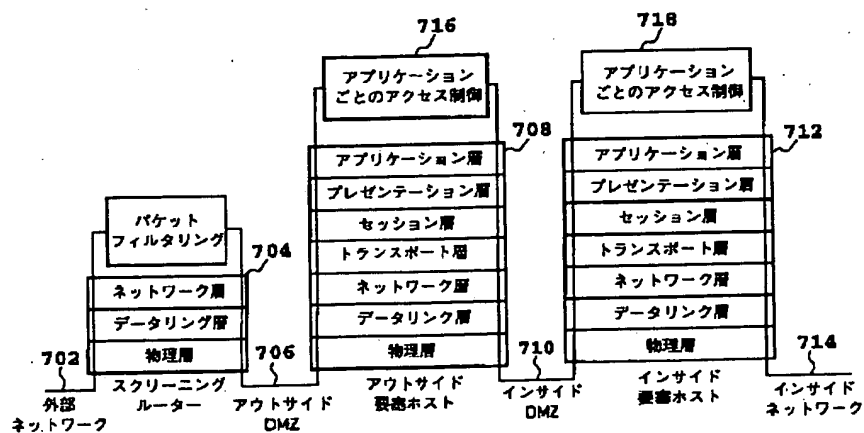
(b)



【図6】



【図8】



【図7】

